2023 新加坡資安交流參訪之觀察與心得

蘇柏鳴 / 金融聯合徵信中心 資安部

隨著日新月異的資訊技術變革，資訊安全已成為全球金融業首要關注的議題，為了提升國內金融業資訊安全的相關能力及國際合作機會，金融研訓院於2023年組織「新加坡資安交流參訪團」，以深化國際間資安領域的交流與合作。

新加坡作為亞洲金融中心，其資安政策、標準和最佳實踐具有廣泛的影響力，透過參訪新加坡的金融機構及資安企業，參訪團成員可以更全面地了解新加坡資安市場的發展情況和前沿動態，本次參訪團將與新加坡當地的資安專家和業界領袖進行深入交流，分享彼此在資訊安全領域的經驗和成果，這將有助於搭建國際間資安合作的橋樑，提升我國金融業在資安領域的國際地位。

本次參訪團將重點關注網路安全、資料安全、人工智能等前沿技術在資訊安全領域的應用，以及銀行如何利用這些技術提升資安水平，新加坡在資訊安全監管方面具有豐富的經驗，參訪團將學習新加坡金融機構在資安風險評估、管理和應對方面的最佳實踐，以期在國內金融業推動資訊安全監管的創新和完善。

本次參訪星展銀行（DBS）、亞馬遜網路服務公司（AWS）以及新加坡在資訊安全相關領域公司，可以透過通過實地考察、座談會和專題講座等多種形式，讓參訪團成員與新加坡資安專家和業界領袖進行互動式交流，藉此更深入地了解新加坡金融科技資安的實際情況，並從中得到寶貴的經驗和建議。

參訪過程

一、AWS（Amazon Web Services）

（一）日期與時間：112年9月5日，09：00~12：00

（二）內容摘要

講授/簡報代表：Reca Kuo、Bard Lan 藍元宏、Patrick Chang、Joseph Wong

1. AWS 共同責任模型

2. 台灣金融法規與雲端服務

（1）風控與監督

AWS 服務建構於完善規劃且高度安全的雲端基礎設施之上全世界最大的雲端基礎架構部署，採用一致的高可用性、可靠、耐用性及低網路延遲架構。

圖一 AWS 共同責任模型[1]

（2）認證及查核

AWS已於2022年度成功完成首次金融聯合查核。

根據「金融機構作業委託他人處理內部作業制度及程序辦法」相關問題適用解說問答集雲端委外，查核範圍應參考ISO27001、ISO27017和雲端安全聯盟（CSA）STAR。

（3）相關申請文件

- ●受委託機構出具之同意函或委外契約，同意必要時得由金融機構指定之人，對受託事項進行查核。
- ●受委託機構出具近三年內未發生造成客戶權益受損或影響機構健全營運之人員舞弊、資通安全及其他事件之聲明書。
- ●作業委外計畫書，其內容應包括： 風險評估及管理機制、客戶資訊保護措施及是否已取得客戶同意、資訊安全及管理、緊急應變計畫，包括受委託機構發生無法提供服務情事或服務中斷之營運備援計畫。

（三）結論與建議

1. 認為「共同責任模型」對於雲端風險管控與建立問責制度的落實有幫助。
2. 大規模實現安全與合規，符合金融機構的需要。

金融機構面臨主管機關的高度監理與合規義務的嚴格要求，AWS與2022年完成首次金融聯合查核，代表對於各金融機構的需求與規範內容有一定程度的了解。

1 AWS 共同責任模型 https：//docs.aws.amazon.com/zh_tw/wellarchitected/latest/security-pillar/shared-responsibility.html

3. 提供個人化、無障礙的體驗，可以滿足金融科技的發展與場景服務。

利用豐富的資料以及人工智慧（AI）和機器學習（ML）的強大功能，為客戶、員工、中介機構和其他利害關係人提供變革體驗。

4. 快速的創新力可以提高金融服務的競爭力。

AWS他們憑藉合作夥伴的社群關係，提供的金融業界最全面的服務和解決方案組合，讓金融服務的構想更快地到轉變為實作。

5. 高效率與敏捷性的特性，更能即刻滿足顧客的瞬間與大量的需求。

6. AWS服務建構於完善規劃且高度安全的雲端基礎設施之上 全世界最大的雲端基礎架構部署，採用一致的高可用性、可靠、耐用性及低網路延遲架構。

AWS在烏俄戰爭期間提供烏克蘭大量重要資料的境外備份需求，這樣的實績有助於台灣在面臨地緣政治的衝突時，也能迅速與大量的備份或備援重要金融機構資料與系統。

二、Panorays

（一）日期與時間：112年9月5日，14：00~15：30

（二）參訪內容摘要

講授/簡報代表：John ONG

1. Panorays產品為自動化、加速和擴展第三方安全評估和管理流程，以便客戶能夠快速輕鬆地管理、減輕和補救風險、減少數據洩露、確保供應商合規並全面改善其網絡安全狀況。
2. 功能包含網絡風險評估、外部攻擊面評估、自動問卷、網絡風險評級等。
3. Panorays供應鏈管控分為四個階段：
   (1)收集本身企業需要的廠商有哪些，然後分出哪些廠商對於企業是重要的。
   (2)評估這些些廠商是否有問題，主要透過兩種方式：
   ●網路上掃描及收集資料
   ●問卷調查
   (3)修復措施：基於發現的資安差距制定修復計畫。
   (4)持續監控：對於重要的供應商的資安態勢和內部安全政策變更持續更新。

（三）結論與建議

1. 「金融機構資通系統與服務供應鏈風險管理規範」第七條 於供應商契約存續期間，應注意下列原則：六、建立對核心資通系統與第一類電腦系統供應商資訊安全稽核之程序，包含稽核結果之改善追蹤機制。依據供應鏈資訊安全風險評估結果選擇合適之資訊安全稽核之方式與頻率，包含自行辦理或委託獨立第三方執行資訊安全訪視作業，或由供應商提供公正第三方之驗證報告。
2. 前述之依據供應鏈資訊安全風險評估結果選擇合適之資訊安全稽核之方式與頻率，可以利用自動化管理方式比較有系統的評估供應鏈的風險，進而訂定稽核方式跟頻率。

三、CyberArk

（一）日期與時間：112年9月5日，16：00~17：40

（二）參訪內容摘要

講授/簡報代表：Edmund Tsui、Jeffrey Kok

1. CyberArk 的沿革及公司介紹，CyberArk 有 Lab 研究駭客如何侵入網路安全的，並提供定期報告。
2. 介紹CISA 提出之Zero Trust Maturity Model（ZTMM）的五個支柱及Zero Trust Architecture Framework （NIST 800-207），如果要做到完整Zero Trust 需要涵蓋整個NIST 800-207的框架，所以比較可行的方式是先從Identity執行。

圖二 Zero Trust Maturity Model（ZTMM）**的五個支柱**

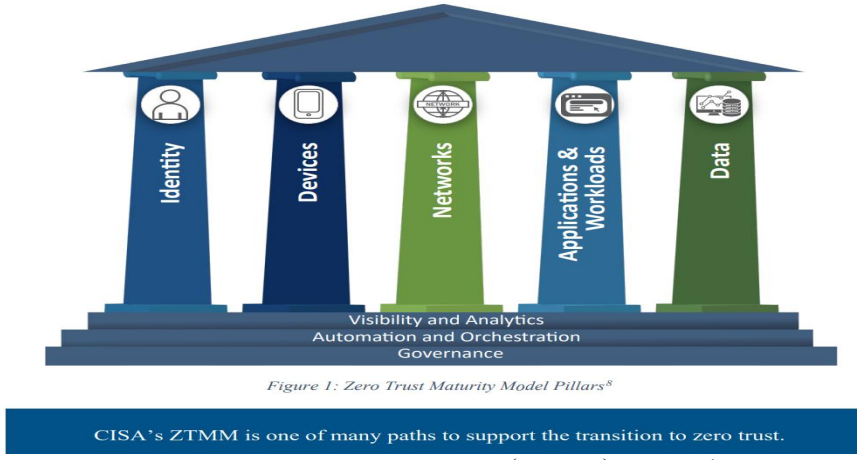
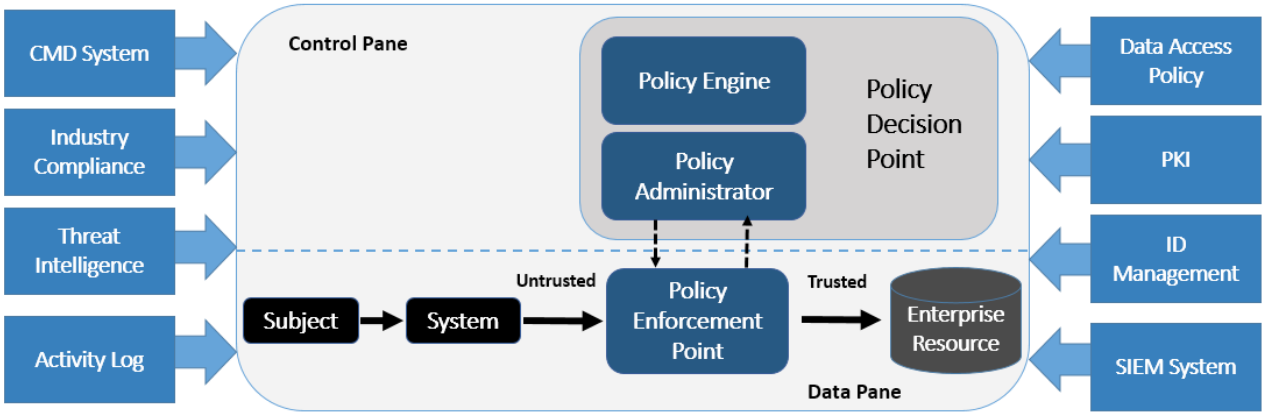


Figure 1: Zero Trust Maturity Model Pillars[8]

圖三 Zero Trust Architecture Framework （NIST 800-207）



3. 端點特權管理系統需要很多Policy去配置，管理面上會有困難，目前CyberArk 透過人工智慧觀察客戶端點上的使用行為，建議或推薦相關Policy 設定，讓防護更有效的幫助客戶。
4. 產品技術相關介紹。

（三）結論與建議

金管會於111年12月27日公布之「金融資安行動方案」2.0中，提到「鼓勵零信任網路部署，強化連線驗證與授權管控」目標，參考行政院「國家資通安全發展方案（110年至113

年）」之推動政府機關導入零信任網路，希望111年完成身分鑑別、112年完成設備鑑別及113年完成信任推斷，感想如下：

1. 零信任屬於架構及生態問題，不是簡單化分成三階段就能確實達到零信任架構。
2. NIST 800-207有提到micro segmentation，該如何落實micro segmentation是ZTA的核心問題。
3. 信任推斷之依據需要許多額外資訊之判斷，例如端點防護資料、弱掃資料…等，各系統串接整合問題及相關資料正規依據。
4. 身分鑑別、設備鑑別及信任推斷，三階段是延續的概念，每個階段環環相扣，應整體一併考量及規劃。

四、星展銀行DBS

（一）日期與時間：112年9月6日，09：30~12：00

（二）參訪內容摘要

講授/簡報代表：Foong Wai Ho

1. 2022年星展銀行再度榮獲美國金融刊物《環球金融》評為全球最佳銀行，這是自2018年以來銀行第三次獲得該雜誌的最高榮譽。
2. DBS裡的資安主管 Mr. Ho 介紹其使用mobile token提升其網路銀行的安全，客戶在申請使用時，經過冷靜期後才能進行轉帳。並在APP上明顯的位置顯示警訊，並且技巧性強迫客戶一定檢視相關訊息。
3. 在高度數位化的資訊服務，運用Block Chain將客戶資訊整合，在推展數位化的同時，為讓提供客戶放心的交易平台，資訊安全是不可或缺的重要一角。
4. 除了透過SIEM平台收集大量Log，並且導入SOAR，運用自動化機制可達到98%以上的自動篩選，減少大量的人工作業。如此完善的機制也是透過長時間的淬鍊才有辦法達成。
5. 與業務單位的密切合作，也是在推展資安過程不可或缺的重要因素，資訊安全的佈建搭配業務的發展，協助業務推展時的安全性，當然還有資訊部門的合作，都是非常重要之因素，這得要有很好的溝通、協同合作並能獲得高層的支持。
6. 整體系統佈建的同時也要能夠考量風險分攤，選擇合作廠商時也要考量儘量分散在不同供應商，就連對自己網站掃描安全性漏洞等檢測軟體，星展銀行就分別與 5家不同廠商合作。
7. 最後實地參觀SOC中心的運作，過程中展示了監控各項網路訊息及系統Log資料分析，也提到監控各項設備的回報率是在監控過程中比較容易被忽略的部分，並且提到充足的人力跟自動化機制才能支撐自建SOC的運作。

（三）結論與建議

1. DBS 設定的目標是類似AWS等這樣的科技公司，而非是傳統的銀行業，依著「以終為始」的精神，朝著目標前進。
2. 另國內目前有些SOC採自建或委外，因人力、場地、技術成熟度等因素考量，而有不同選擇，總之為所屬機構找合適的運作方式，就是最好的解決方案。

3. 星展銀行能夠發展至如此完善的規模，是我們學習的目標及未來發展框架的借鏡，但萬丈高樓平地起，我們必須思考策略目標在何處，若能結合從業務運行順利且安全的角度溝通資訊安全投資所帶來的價值，才在組織內順利推動。
4. 此行的參訪與DBS的資安團隊交流外，也增加與本國金融機構更多的交流機會，也體會了資安聯防的重要，在國內的金融機構目前尚未有百人以上的專職資安團隊，不過可經由資安聯防合作來彌補各別機構的不足。

五、FS-ISAC

（一）日期與時間：112年9月6日，14：00~15：40

（二）參訪內容摘要

講授/簡報代表：Chris Wong、Andy Chow、Jaron Hwee、Christophe Barel、Heidi Tan

1. 有關整體網路安全概況趨勢，包含以下重點：
   (1)惡意軟體市場快速增長，已經成為一項服務，由於能見度增加、對惡意軟體服務需求上升以及AI技術進步等原因，網路攻擊變得更容易，威脅攻擊者越來越專業化，並銷售他們的專業知識。而供應鏈的資安威脅，亦是另一個需要注意的議題。
   (2)AI技術可以強化網路安全，並減少低複雜性環境下所需的人力，但相對的也將進一步威脅網路安全。另加密貨幣的使用正在改變網路安全格局，與網路犯罪相關的戰術也在不斷演變。未來可能會看到更多的AI和雲端計算在威脅情資中的應用，而量子計算帶來了密碼學的挑戰，組織必須為潛在威脅做好準備。
   (3)機器學習演算法可以分析大量資料以識別模式，有助於威脅偵測與回應。金融機構面臨著越來越多的監管、網路保險的不確定性和網路安全人才短缺，新技術如AI將在網路安全中發揮關鍵作用。群體合作、分享最佳實踐和行業指引對金融機構的安全至關重要。網路威脅將繼續多樣化和自動調適以找到防禦漏洞，因此組織必須不斷強化網路安全態勢，包括掌握威脅情資、共享資訊和攻防演練等。
   (4)組織必須就資安事件做好準備，並理解完全預防是不可能的，除了事後快速反應外，事前的準備對增強營運韌性也至關重要。詐騙正在不斷演變，需要創建綜合的、面向整個行業的能力來對抗廣泛傳播的攻擊。保護消費者、自我調整防禦和新興威脅類型變得更為重要，FS-ISAC將透過加強情資維運和網路安全專業知識來提高應對能力。
2. 有關避風港計畫，包含以下重點：
   (1)避風港當初的目的，是在確保金融機構客戶的資產，不會因為重大災害或網路攻擊而消失。並能在事故發生的24小時內，提供查詢或基本的資金調撥。
   (2)避風港計畫主要是透過三個面向來達成，首先是資料儲存庫（data vaulting），也就是將客戶帳戶重要資料進行備份，並將資料存放於儲存庫中。

第二則是要擬定復原計畫（resilience planning），確保災害或事故發生時，組織可依計畫程序快速進行資料復原及提供服務。最後則是認證，其在確保相關機制或設施的有效性。

(3)有關資料的備份，金融機構將於每天晚上針對重要客戶帳戶資料及額外補充資料進行備份，且將先經資料加密再存放至儲存庫中。儲存庫將具備不可異動（immutable）、實體隔離（air-gap）及去中心化（de-centralized），並且由金融機構所控管。

(4)復原計畫則包含復原的標的、事故的管理、危機溝通等等，相關的計畫必須經過測試及驗證，以利事故發生時，能透過備份的資料及復原程序，於原訂的復原平台上，提供必要的金融服務。

(5)原避風港計畫僅專注於重要的客戶帳戶資料，然而對金融機構而言，實際還有其他重要的資料，也可以透過此機制來妥善保護。因此新的規格，將不再僅限客戶帳戶資料，而延伸至可安全儲存及回復金融機構的重要資料。

3. 有關新加坡的網路安全概況，包含以下重點：

(1)2022年新加坡4大主要威脅項目的趨勢，網路釣魚（phishing attempt）大幅增長了2倍；勒索軟體（ransomware）雖然下降4%，但仍然維持很高；感染的基礎設施（infected infrastructure）下降了13%，主要是因為網路衛生水平提高；網頁置換（website defacement）下降了19%，可能是轉到其他平台。

(2)新加坡上半年詐騙受害者損失3.345億新幣[2]，新加坡警政透過分享知識（認知）、成立反詐騙指揮部，過濾可疑的簡訊訊息，移除簡訊及電子郵件中的可點擊連結，並由政府提供防詐工具（ScamShield[3]）等多管齊下來防止詐騙的發生。

4. 有關金融機構韌性概述，包含以下重點：

(1)透過演練、訓練及腳本，金融機構可以建立對網路攻擊回應的具體程序及提升反應效率，而FS-ISAC提供演練（如網路攻防演練、桌面演練等）、事件應變（如事件發生後的支援、事件應變腳本制定等）、關鍵供應商計畫及業務韌性委員會。

(2)建立全球韌性網絡，利用即時資訊網路系統，共享相關情資。

(3)為會員提供桌面演習和網路攻擊演習，並代表金融部門，定期參加一些全球和地區性演習。如CAPS Exercises即是桌面演習，而Cyber-Range Exercises則為網路攻擊演習。另外和美國、英國以及與北約開展公私合作演習的經驗，且將在今年於亞太地區組織一次公私合作演習。

2 新加坡上半年詐騙受害者損失 3、345 億新元 https：//www.fx110.com.tw/special/11294

3 https：//www.scamshield.org.sg/

（三）結論與建議

1. 隨著攻擊工具或服務商品化，金融機構面對的網路威脅也將越多越即時，當攻擊者也將AI/ML作為其攻擊工具時，金融機構亦應思考善用自動化機制或AI/ML來因應。
2. 量子運算對密碼學的影響似乎已經迫在眉睫，尤其非對稱加解密演算法如RSA等，目前正廣泛應用於金融業的高風險交易，故其衝擊將相當大。金融同業應盡快盤點目前各交易使用的密碼學演算法，識別出量子運算影響的演算法，並研議後續如何調整或因應。
3. 避風港是一套完整的跨機構的資料備份與基本服務復原計畫，雖然國內目前並未有類似計畫，但金融資安行動方案2.0亦提到「深化核心資料保全及營運持續演練」，現行金融機構可參考避風港計畫中資料備份的安全機制，以強化資料保全的安全。
4. 有關詐騙的防範，除了對一般大眾的宣導外，新加坡直接由政府介入，於技術上提供防範的應用程式，並於可疑的簡訊及電子郵件上直接移除惡意的連結，其在安全防護上能有最直接快速的效果，或許可成為我們的借鏡。
5. 資安防護並無法做到滴水不漏，如何於事件發生後能快速因應與復原，才是維持金融韌性的重要關鍵。金融資安行動方案2.0亦提到「精實金融機構資安作業韌性」，其中包含「增進金融機構營運持續管理量能」及「加強資安演練」，有關資安演練部分，FS-ISAC涵蓋相關完整，包含桌面及網路實戰演練，且具跨國、區域的演練實務經驗，可參考其演練的方式，持續強化國內演練的有效性。

心得及建議

很感謝聯徵中心給予參加「新加坡資安交流參訪團」的機會，雖然此次參訪行程時間較短，但內容卻很充實，本次行程印象最深刻的是參訪DBS跟AWS的行程，在參訪過程中見識到DBS憑藉高度自動化的系統整合，讓只有20幾個人的團隊能24小時監控DBS全球的資安告警，其中利用自動學習的方式避開大量告警雜訊，讓監控人員可以專注那些有意義的告警內容，做到人力的有效運用，這個過程他們也花了7年多的時間才完成。

另外參訪AWS過程中詳細說明他們對於先進國家法規對於雲端業者要求的應對方式，說明雲端業者也很重視法規限制帶來的雲端業務推動的影響，此次的收穫讓我之後對於後續ZTA、雲端服務跟MDA戰情室規規劃等業務有實質上的啟發，除此之外，這次團員臥虎藏龍，讓我在跟團員交流中受益良多，並且建立之後與銀行資安交流管道，以利未來面對新的資安議題可以有更多的參考來源。